

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Manxia Tie et al.

Application No.: 10/534,067

Confirmation No.: 2699

Filed: January 17, 2006

Art Unit: 2431

For: A METHOD FOR THE ACCESS OF THE
MOBILE TERMINAL TO THE WLAN AND
FOR THE DATA COMMUNICATION VIA
THE WIRELESS LINK SECURELY

Examiner: Jeremiah L. Avery

RESPONSE AFTER FINAL OFFICE ACTION

MS AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

INTRODUCTORY COMMENTS

In response to the Office Action dated April 23, 2010, please consider the following remarks:

A Listing of the Claims begins on page 3 of this paper.

Remarks/Arguments begin on page 13 of this paper.

OK TO ENTER: /J.A./

FEE CALCULATION

Any additional fee required has been calculated as follows:

	Claims Remaining After Amendment	Highest Number Previously Paid	Number Extra Claims Present	Rate	Additional Fee
Total	21	- 21 =		X 52.00	
Independent	1	- 3** =		X 220.00	
First presentation of Multiple Dependent Claim(s) (if applicable)					
TOTAL					

*not less than 20

** not less than 3

No additional fee is required.

In the event a fee is required or if any additional fee during the prosecution of this application is not paid, the Patent Office is authorized to charge any underpayment or credit any overpayment to Deposit Account No. 50-2215.

CONTINGENT EXTENSION REQUEST

If this communication is filed after the shortened statutory time period had elapsed and no separate Petition is enclosed, the Commissioner of Patents and Trademarks is petitioned, under 37 CFR 1.136(a), to extend the time for filing a response to the outstanding Office Action by the number of months which will avoid abandonment under 37 CFR 1.135. The fee under 37 CFR 1.17 should be charged to our Deposit Account No. 50-2215.

LISTING OF THE CLAIMS

1. (Previously Presented) A method for the secure access of a mobile terminal to a Wireless Local Area Network (WLAN) and for secure data communication via wireless link, wherein when a Mobile Terminal (MT) logs on a wireless Access Point (AP), a Mobile Terminal (MT) certificate and an Access Point (AP) certificate are transmitted to an Authentication Server (AS) and are authenticated through the Authentication Server (AS), then the authentication result of the Mobile Terminal (MT) certificate and the Access Point (AP) certificate is returned to the Access Point (AP) and the Mobile Terminal (MT) in order to achieve the direct two-way certificate authentication between said Mobile Terminal (MT) and Access Point (AP); and the Mobile Terminal (MT) and the Access Point (AP) perform negotiation of secret key for conversation.

2. (Original) The method for the secure access of mobile terminal to the Wireless Local Area Network (WLAN) and for secure data communication via wireless link according to claim 1, wherein:

when MT logs on AP, MT and AP performs said two-way certificate authentication through AS;

after said two-way certificate authentication is successfully performed, MT and AP perform said negotiation of the secret key for conversation.

3. (Previously Presented) Said method for the secure access of mobile terminal to the Wireless Local Area Network (WLAN) and for secure data communication via wireless link according to claim 1, wherein:

when MT logs on AP, MT and AP inform one another of their respective certificate, and then they perform negotiation of secret key for conversation;

after said negotiation of secret key for conversation is completed, MT and AT performs the two-way certificate authentication through AS, and meanwhile judge whether the certificate used by the other part is the same as the one informed by it such that if it is not the same, the authentication fails; if it is the same, the result of the authentication depends on the result of said two-way certificate identification.

4. (Previously Presented) The method for the secure access of mobile terminal to the Wireless Local Area Network (WLAN) and for secure data communication via wireless link according to claim 1, wherein: said two-way certificate authentication comprising the steps:

1) when MT logs on AP, MT sends to AP the access authentication request message containing the MT certificate;

2) after AP receives said access authentication request message, it adds the AP certificate to the message, then sends to AS the certificate authentication request message containing said MT certificate and AP certificate;

3) after AS receives said certificate authentication request message, AS authenticates the AP certificate and MT certificate in said message, and then sends back to AP the certificate authentication response message containing the AS signature;

4) after AP receives said certificate authentication response message, AP authenticates the AS signature, so as to obtain the result of authentication of the MT certificate, and then sends back to MT the certificate authentication response message as the access authentication response message; and

5) after MT receives said access authentication response message, MT authenticates the AS signature and obtains the result of authentication of the AP certificate, so as to complete said two-way certificate identification between MT and AP.

5. (Original) Said method for the secure access of mobile terminal to the Wireless Local Area Network (WLAN) and for secure data communication via wireless link according to claim 1, wherein:

1) when MT logs on AP, MT sends to AP the access authentication request message containing the MT certificate for said two-way certificate authentication;

2) after AP receives said access authentication request message, it adds the AP certificate to the message, then sends to AS the certificate authentication request message containing said MT certificate and AP certificate for said two-way certificate authentication, and meanwhile begins with MT negotiation of the secret key for conversation;

3) after AS receives said certificate authentication request message, AS authenticates the AP certificate and MT certificate in said message, and then sends back to AP the certificate authentication response message containing AS signature for said two-way certificate authentication;

4) after AP receives said certificate authentication response message, AP authenticates the AS signature, so as to obtain the result of authentication of the MT certificate, and then sends back to MT the certificate authentication response message as the access authentication response message for said two-way certificate authentication; and

5) after MT receives said access authentication response message, MT authenticates the AS signature and obtains the result of authentication of the AP certificate, so as to complete the process of said two-way certificate identification between MT and AP, and then MT performs the corresponding processing to complete said negotiation of secret key for conversation.

6. (Original) The method for the secure access of mobile terminal to the Wireless Local Area Network (WLAN) and for secure data communication via wireless link according to claim 1, wherein:

1) when MT logs on AP, MT sends AP the access authentication request message containing the MT certificate for said two-way certificate authentication;

2) after AP receives said access authentication request message, it adds the AP certificate to the message, then sends to AS the certificate authentication request message containing said MT certificate and AP certificate for said two-way certificate authentication;

3) after AS receives said certificate authentication request message, AS authenticates the AP certificate and MT certificate in said message, and then sends back to AP the certificate authentication response message containing AS signature for said two-way certificate authentication;

4) after AP receives said certificate authentication response message, AP authenticates the AS signature, so as to obtain the result of authentication of the MT certificate, AP judges the result of authentication. If the authentication is not successful, AP sends back to MT said certificate authentication response message as the access authentication response message for said two-way certificate authentication; If the authentication is successful, AP begins to consult with MT the secret key for to conversation while it sends back to MT said access authentication response message; and

5) after MT receives said certificate authentication response message, MT authenticates the AS signature and obtains the result of authentication of the AP certificate, so as to complete said two-way certificate identification between MT and AP, and then MT performs the corresponding processing to complete said process of negotiation of secret key for conversation.

7. (Previously Presented) The method for the secure access of mobile terminal to the Wireless Local Area Network (WLAN) and for secure data communication via wireless link according to claim 1, wherein:

1) when MT logs on AP, each part informs the other of its own certificate, then they complete said negotiation of secret key for conversation, and, meanwhile, MT also completes informing AP of the access authentication request identification;

2) AP sends to AS the certificate authentication request message containing the MT certificate and AP certificate for said two-way certificate Authentication;

3) after AS receives said certificate authentication request message, AS authenticates the AP certificate and MT certificate in said message, and then sends back to AP the certificate authentication response message containing AS signature for said two-way certificate authentication;

4) after AP receives said certificate authentication response message, AP authenticates the AS signature, so as to obtain the result of authentication of the MT certificate, and then sends back to MT said certificate authentication response message as the access authentication response message for said two-way certificate authentication; and

5) after MT receives said access authentication response message, MT authenticates the AS signature, and then judges whether the AP certificate is the same as the one AP informed of before negotiation of secret key for conversation such that if it is not the same, the authentication fails; if it is the same, MT obtains the result of the authentication of the AP certificate from the message, so as to complete said two-way certificate authentication process between MT and AP.

8. (Previously Presented) The method for the secure access of mobile terminal to the Wireless Local Area Network (WLAN) and for secure data communication via wireless link

according to claim 1 wherein: said access authentication request message also comprising the access authentication request identification.

9. (Previously Presented) The method for the secure access of mobile terminal to the Wireless Local Area Network (WLAN) and for secure data communication via wireless link according to claim 1, wherein: said certificate authentication request message also comprising the access authentication request identification, or also comprising the access authentication request identification and AP signature.

10. (Previously Presented) The method for the secure access of mobile terminal to the Wireless Local Area Network (WLAN) and for secure data communication via wireless link according to claim 1, wherein: said certificate authentication response message also comprising, before the signature filed of AS, the information of the result of the MT certificate authentication and those of the AP certificate authentication.

11. (Previously Presented) The method for the secure access of mobile terminal to the Wireless Local Area Network (WLAN) and for secure data communication via wireless link according to claim 1, wherein: said access authentication response message is identical with said certificate authentication response message.

12. (Previously Presented) The method for the secure access of mobile terminal to the Wireless Local Area Network (WLAN) and for secure data communication via wireless link according to claim 1 wherein: said access authentication request identification is a string of random data or authentication serial number.

13. (Previously Presented) The method for the secure access of mobile terminal to the Wireless Local Area Network (WLAN) and for secure data communication via wireless link according to claim 1, wherein: said information of MT certificate authentication result comprising the MT certificate, and the MT certificate authentication result and the AS signature, or comprises the MT certificate and the MT certificate authentication result.

14. (Previously Presented) The method for the secure access of mobile terminal to the Wireless Local Area Network (WLAN) and for secure data communication via wireless link according to claim 1, wherein: said information of the AP certificate authentication result comprises the AP certificate, the AP certificate authentication result, the access authentication request identification and the AS signature, or comprises the AP certificate, the AP certificate authentication result and the access authentication request identification.

15. (Previously Presented) The method for the secure access of mobile terminal to the Wireless Local Area Network (WLAN) and for secure data communication via wireless link according to claim 1, wherein; when MT intends to access to the designated AP, the MT must first of all obtain the relevant information of the AP or the certificate of the AP.

16. (Previously Presented) The method for the secure access of mobile terminal to the Wireless Local Area Network (WLAN) and for secure data communication via wireless link according to claim 1, wherein: said negotiation of secret key for conversation refers to MT or AP using AP's or MT's common key and their respective own private key to generate the secret key for conversation.

17. (Previously Presented) The method for the secure access of mobile terminal to the Wireless Local Area Network (WLAN) and for secure data communication via wireless link according to claim 1, wherein: said negotiation of secret key for conversation comprising:

1) MT secretly chooses an integer a , from which to calculate the integer $f(a)$, combines the integer $f(a)$ and the MT signature on it into the secret key negotiation request message, and transmits it to AP; said f is a function rendering integer a from the integer $f(a)$ in calculable;

2) after it receives said secret key negotiation request message, AP secretly chooses an integer b , from which to calculate the integer $f(b)$, combines the integer $f(b)$ and the AP signature on it into the secret key negotiation response message, and transmits it to MT; said f is a function rendering integer b from the integer $f(b)$ in calculable; and

3) AP calculates $g(b, f(a))$, and MT calculates $g(a, f(b))$ after it receives said secret key negotiation response message, as the secret key for conversation in the process of communication; said g is a function rendering the calculation of $g(a, f(b))=g(b, f(a))$ possible.

18. (Previously Presented) The method for the secure access of mobile terminal to the Wireless Local Area Network (WLAN) and for secure data communication via wireless link according to claim 1, wherein: said negotiation of secret key for conversation comprising:

1) AP secretly chooses an integer b , from which to calculate integer $f(b)$, combines the integer $f(b)$ and the AP signature on it into the secret key negotiation request message, and transmits it to MT; said f is a function rendering integer a from the integer $f(b)$ in calculable;

2) after it receives said secret key negotiation request message, MT secretly chooses an integer a , from which to calculate the integer $f(a)$, forms the integer $f(a)$ and the MT signature on it into the secret key negotiation response message, and transmits it to AP; said f is a function rendering integer a from the integer $f(a)$ in calculable; and

3) MT calculates $g(a, f(a))$, and AP calculates $g(a, f(b))$ after it receives said secret key response message, as the secret key for conversation in the process of communication; said g is a function rendering the calculation of $g(a, f(b))=g(b, f(a))$ possible.

19. (Previously Presented) The method for the secure access of mobile terminal to the Wireless Local Area Network (WLAN) and for secure data communication via wireless link according to claim 1, wherein: said negotiation of secret key for conversation comprising:

1) MT or AP generates a string of random data, and sends them to AP or MT as the secret key negotiation request message after encryption using the common key of AP or MT;

2) After it receives said secret key negotiation request message from MT or AP, AP or MT uses its own private key for decryption, obtains the random data generated by the other part; then AP or MP generates again a string of random data; and sends them to MT or AP as the secret key negotiation response message after encryption using the common key of MT or AP; and

3) After it receives said secret key negotiation response message from AP or MT, MT or AP, uses its own private key for decryption, obtains the random data generated by the other part; both MT and AP utilizes the random data generated by the other part and itself to generate the secret key for conversation.

20. (Previously Presented) The method for the secure access of mobile terminal to the Wireless Local Area Network (WLAN) and for secure data communication via wireless link according to claim 1, wherein: said negotiation of secret key for conversation comprising:

1) MT or AP generates a string of random data, and, after it utilizes the common key of AP or MT for encryption, attaches its own signature as the secret key negotiation request message, and transmits it to AP or MT; and

2) after AP or MT receives said secret key negotiation request message from MT or AP, it utilizes the common key of MT or AP to authenticate the signature, and then utilizes its own private key to decrypt the encrypted message received; both MT and AP uses the random data as the secret key for conversation.

21. (Previously Presented) The method for the secure access of mobile terminal to the Wireless Local Area Network (WLAN) and for secure data communication via wireless link according to claim 1, wherein: said negotiation of secret key for conversation also comprising negotiation of the communication algorithm used in the process of communication.

REMARKS

Claims 1-21 are pending. Claim 1 is the only independent claim. Favorable reconsideration is respectfully requested.

Claims 1-16 and 19-21 were rejected under 35 U.S.C. § 103 over U.S. Patent 7,350,076 (Young et al.) in view of U.S. Patent Publication 2004/0103283 (Hornak). Claims 17 and 18 were rejected under 5 U.S.C. § 103 over Young et al. and Hornak, and further in view of U.S. Patent 5,515,439 (Bantz et al.). Applicants submit that independent claim 1 is patentable over the cited art for at least the following reasons.

The Office Action conceded that Young failed to disclose the feature “wherein when a mobile terminal (MT) logs on a wireless Access Point (AP), a Mobile Terminal (MT) certificate and an Access Point (AP) certificate are transferred to an Authentication server (AS)...in order to achieve the direct two-way certificate authentication between said Mobile Terminal (MT) and Access Point (AP)” of claim 1. However, the position was taken that such features are taught by Hornak. Applicants disagree.

The authentication process of Hornak can be divided into two phases, with the first phase relating to authentication during the certificate issuance process and the second phase relating to authentication when the communication entities use the certificates. In the first phase, the trusted third party CA is responsible for certificate issuance to the three entities such as Client, Gateway and Origin Server respectively (see, e.g., Hornak, paragraphs 0014 and 0084). Authentication in this phase will guarantee that the certificates obtained by the three entities are authenticated and signed by the Certification Authority CA. Paragraph 0083 of Hornak, identified by the examiner, describes the authentication process in this first phase.

During the second phase, the Client communicates with the Gateway under a certain protocol to exchange certificates with each other. Each party authenticates the formality correctness of the other's certificate according to the public key (CA-PK) of CA included thereof and obtains the public key information of the other party. In particular, the Gateway obtains the public key of the client (C-PK) and the Client obtains the public key of the Gateway (G-PK). Thereby the two

way authentication is achieved. Depending on the other party's public key information, the two parties negotiate the master key for communication and start private communication using WTLS. (See, e.g., Hornak, paragraph 0013; paragraph 110). Similar protocol exchange as that between the Client and the Gateway is made between the Gateway and the Original Server and private communication using SSL or TLS begins after the master key is negotiated. (See, e.g., Hornak, paragraphs 111-114). Therefore, according to Hornak, during the second phase when certificates are in use, certificates authentication is accomplished by exchanging certificates between the two communication entities. (See, e.g., Hornak, lines 12-15 of paragraph 0014; lines 1-5 of paragraph 0021).

According to the solution of Hornak, by authentication in the certificate issuance process (corresponding to the first phase), any user can authenticate whether the certificate is issued by the alleged issuer based on the information of the issuer (normally means the public key information of the issuer). However, in practice, the public key certificate owned by a device as its unique identifier can be revoked or becomes invalid due to divulgence of the private key or other reasons. If the invoked or invalidated certificates are still in use, secure communication between two parties can not be guaranteed. Unfortunately, the solution of Hornak cannot address this problem since it presumes any certificate in use is valid as far as it has been authenticated in the issuance phase. In Hornak, during the second stage, authentication is achieved simply by exchanging the certificates between the two entities.

Claim 1 solves this problem and achieves real-time authentication of the certificates not only regarding formality, but also validity when they are in use. Compared with Hornak the invention of claim 1 focuses on the second phase authentication and takes a different authentication solution in this phase. In particular, claim 1 makes use of the trusted third party---Authentication Server -- to authenticate the status of the certificates in order to achieve real-time and flexible management of the devices. According to the technical feature "the Mobile Terminal (MT) certificate and the Access Point (AP) certificate are transmitted to the Authentication Server (AS) and are authenticated through the Authentication Server (AS)" in claim 1, the Authentication Server authenticates not only the formality but also the status validity of the certificates. Therefore, it can

make real-time judgment about whether the identities of the mobile terminal MT and the wireless access point AP are legal.

The authentication of the certificates by the Authentication Server of the claimed invention is not equivalent to the formality authentication of the certificates exchanged between the Gateway and Client by authenticating the signature portions of the other party defined in Hornak. Although it might seem in Hornak the two parties also perform two way certificate authentication, in fact only the formality of the other party's certificate is authenticated by each party, instead of the legal status of the certificates. Therefore, the object of authentication has not been achieved. Consequently, it cannot be guaranteed that the legal user is using the legal network.

With reference to Fig. 5 of Hornak and the corresponding description, it will be easy for the person skilled in the art to understand that what is described in paragraph 0083 (on page 5): “[T]he CA 48 is accessible by the client 42, the origin server 44 and the gateway 46 for authentication of a certificate belonging to each of these parties” is different from the definition “when a Mobile Terminal (MT) logs on a wireless Access Point (AP), the Mobile Terminal (MT) certificate and the Access Point (AP) certificate are transmitted to the Authentication Server (AS) and are authenticated through the Authentication Server (AS)” of claim 1.

In Hornak, during the certificate issuance stage (first phase), CA issues signed certificates to the three entities Client, Gateway and Original Server. However, in the claimed invention, AS authenticates the certificates of the MT and AP “when Mobile Terminal (MT) logs on wireless Access Point (AP)” (claim1).

Furthermore, the description of Hornak’s paragraph 110 (on page 6): “a protocol handshake is executed between the client 42 and the gateway 46” is different from what is defined in claim 1: “then the authentication result of the Mobile Terminal (MT) certificate and the Access Point (AP) certificate is returned to the Access Point (AP) and the Mobile Terminal (MT) in order to achieve the direct two-way certificate authentication between said Mobile Terminal (MT) and Access Point (AP)”. It can be seen, in Hornak, that when the certificates are in use (second phase), certificates exchange, formality authentication of the certificates and negotiation of the communication master key are all performed between the two entities Client and the Gateway and

do not involve the CA. While in the claimed invention, with three entities involved at this stage, AS returns the authentication results to the Access Point and the Mobile Terminal. Thereby mutual authentication between MT and AP are achieved by the involvement of AS.

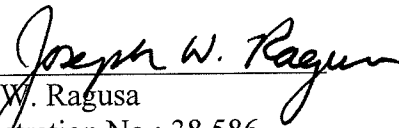
In summary, applicants submit that Hornak fails to disclose or suggest the technical features of the claimed invention as alleged in the Office Action.

For at least the foregoing reasons, claim 1 is believed clearly patentable over Young et al. and Hornak. The dependent claims are believed patentable for at least the same reasons as claim 1. The other references are not believed to remedy the abovementioned deficiencies of the cite art.

In view of the above remarks, applicants believe the pending application is in condition for allowance.

Dated: June 22, 2010

Respectfully submitted,

By 
Joseph W. Ragusa
Registration No.: 38,586
DICKSTEIN SHAPIRO LLP
1633 Broadway
New York, New York 10019-6708
(212) 277-6500
Attorney for Applicant